Notice of Allowability	Application No. 09/303,561	Applicant(s) MORISHITA, TAKUYA	
	Examiner Ronald Baum	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *7/12/04*.

2. ☒ The allowed claim(s) is/are *1-9*.

3. ☐ The drawings filed on _____ are accepted by the Examiner.

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)
1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *08252004* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with David A. Blumenthal, Reg. No. 26,257 on 9/01/2004.

1. Replace claims 1-3 with:

1. A cryptosystem key updating system for preventing illegal use of software, comprising:

encryption means for encrypting secret information;

secret information storage means for storing the secret information;

cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means;

illegal access determining means for determining whether an illegal access to the system is performed; and

cryptosystem key updating means for:

providing the updated same key for a first cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a second cryptosystem key which is stored as an updated cryptosystem key in the cryptosystem key storage means if the illegal access determining means detects no illegal access;

providing different keys for the first and second cryptosystem keys if the illegal access determining means detects an illegal access; and

wherein the cryptosystem key updating means updates the first and second cryptosystem keys for each access to the system, and

subsequently reencrypts the secret information stored in the secret information storage means using the updated first cryptosystem key.

2. A cryptosystem key updating method for preventing illegal use of software, the method used in a system which comprises a means for encrypting secret information; secret information storage means for storing the secret information and a cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means, the method comprising the steps of:

determining whether an access to the system is performed;

and for each access to the system,

providing the same updated key for a first cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a second cryptosystem key which is stored as an updated cryptosystem key in the cryptosystem key storage means if no illegal access is detected in the step of determining whether an illegal access to the system is performed;

providing different updated keys for the first and second cryptosystem keys if an illegal access is detected in the step of determining whether an illegal access to the system is performed; and

subsequently reencrypting the secret information stored in the secret information storage means using the updated first cryptosystem key.

3. A storage medium storing a computer-executable cryptosystem key updating program for preventing illegal use of software, the program used in a system which comprises means for encrypting secret information; a secret information storage means for storing secret information and a cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means, the program including the processes of:

determining whether an illegal access to the system is performed; and

for each access to the system,

providing the same updated key for a first cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a second cryptosystem key which is stored as an updated cryptosystem key in the cryptosystem key storage means if no illegal access is detected in the step of determining whether an illegal access to the system is performed;

providing different updated keys for the first and second cryptosystem keys if an illegal access is detected in the step of determining whether an illegal access to the system is performed; and

subsequently reencrypting the secret information stored in the secret information storage means using the updated first cryptosystem key.

Examiner's Statement of Reasons for Allowance

2. Claims 1-9 are allowed over prior art.

3. This action is in reply to applicant's correspondence of 12 July 2004 and 27 August 2004.

4. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.

5. As per claims 1-3, prior art of record, Atalla, U.S. Patent 4,588,991 fails to teach, alone, or in combination, of;

(claim 1) "A cryptosystem key updating system for preventing illegal use of software, comprising:

encryption means for encrypting secret information;

secret information storage means for storing the secret information;

cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means;

illegal access determining means for ***determining whether an illegal access*** *to the system is performed*; and

cryptosystem ***key updating*** means for:

providing the updated ***same key*** *for a first cryptosystem key used* ***for reencrypting*** the secret information stored in the secret information storage means and a *second cryptosystem key which is stored as* ***an updated cryptosystem key*** in the cryptosystem key storage means *if the illegal access determining means detects* ***no illegal access***;

providing ***different keys*** for the *first and second cryptosystem keys if the illegal access determining means detects* ***an illegal access***; and

wherein the cryptosystem key updating means *updates the first and second cryptosystem keys for* ***each access to the system***, and

subsequently ***reencrypts*** *the secret information stored in the secret information storage means using the updated first cryptosystem key*"

(claim 2-3) whereas the claim 1 equivalent elements for the method and software rendered methods arguments are the same as for claim 1.

The *italicized* above claim elements dealing with "*illegal access determining means for* ***determining whether an illegal access*** *to the system is performed... cryptosystem* ***key updating...*** *providing the updated* ***same key*** *for a first cryptosystem key used* ***for reencrypting...*** *second cryptosystem key which is stored as* ***an updated cryptosystem key...*** *if the illegal access determining means detects* ***no illegal access***; *providing* ***different keys...*** *updates the first and second cryptosystem keys for* ***each access to the system...*** ***reencrypts*** *the secret information stored in the secret information storage means using the updated first cryptosystem key* " serving to patently distinguish the invention from prior art. Specifically, the use of *cryptosystem* ***key updating*** *providing an updated* ***key for reencrypting*** *if the illegal access determining means detects* ***no illegal access*** is taught in the prior art. However, as per the applicants arguments in the previous remarks in the Amendment (July 12, 2004), the examiner finds the applicant's arguments to be persuasive in that the reencryption with a different key upon illegal access determined (versus just doing nothing (i.e., inherent denial of any access) upon illegal access determined, as per the prior art of record), for the purpose of both preventing illegal access to stored software, and continued secure storage of such as a result of the reencryption per se, patently distinguishes the invention from prior art.

Dependent claims 4-9 are allowable by virtue of their dependencies.

Conclusion

6. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100